

## DISTRIBUTIVE GRUPPEN ENDLICHER ORDNUNG

## FINITE DISTRIBUTIVE GROUPS

BURSTIN, C. &amp; MAYER, W.

ABSTRACT. This is a translation of [1]. I have added translations for (possibly) outdated definitions in an appendix at the end.

In this paper, we define distributive groups and show some properties of them. We then concern ourselves with the homogeneity of distributive groups, before showing how they can be generated from both associative and distributive groups. After that, we look at subgroups and define an index theorem for distributive groups before describing the structure of distributive groups. Finally, we present two addenda with several theorems that we proved while trying to prove that  $|(A.p).(A.q)| = |A|$ .

## 1. THE AXIOMATIC OF DISTRIBUTIVE GROUPS

Let there be a system of finitely or infinitely many elements:

$$a \ b \ c \ \dots$$

and a composition that for two elements  $a, b$  in a certain order  $a, b$  assigns the element  $a.b$ , the result of the composition of  $a$  and  $b$ . If the following three Axioms hold, we call such a system a *distributive group*.

- I. Axiom The composition result  $a.b$  of any two elements  $a$  and  $b$  of the system is itself an element of the system.
- II. Axiom If  $a$  and  $b$  are any two elements of the system, then the two equations

$$a.x = b \text{ and } y.a = b$$

have exactly one and only one solution in the system.

(Thus, this Axiom requires the existence and uniqueness of the inverse operations).

- III. Axiom Let  $a, b$  and  $c$  be any three elements of the system then there exist the following two, identical relations

$$(a.b).c = (a.c).(b.c) \text{ and } c.(a.b) = (c.a).(c.b)$$

Axioms I and II are Axioms of classical group theory; instead of Axiom III we have the Axiom of associative composition:  $(a.b).c = a.(b.c)$ . Thus, in order to distinguish them from distributive groups, we will call the classical groups *associative* groups.

---

*Date:* Received November 1927.

If there exists such an Axiomatic system, the questions of independence and (non-) contradiction of the Axioms naturally arise. We show the independence of Axiom I from Axioms II and III:

Let the system of elements be the (positive and negative) integers; let the composition be  $a.b = \frac{a+b}{2}$ . Here, Axioms II and III hold but Axiom I does not.

In a system of *finitely many* elements, Axiom I follows from II.

A second example shows the independence of Axiom II from Axioms I and III.

Let the system consist of  $n$  elements,  $a_1, a_2, \dots, a_n$  and let the composition be  $a_i.a_k = a_k$ . Here, Axioms I and III hold but Axiom II does not.

Every associative group with more than one element is an example for the independence of Axiom III from the other two. For this, we will show that such an associative group cannot be distributive.

The non-contradiction of the Axioms is shown by the creation of distributive groups in the following examples:

- (1) Let the system of elements be the complex numbers. To the numbers  $a$  and  $b$ , the composition  $a.b$  shall assign the number

$$a.b = \alpha a + \beta b$$

where  $\alpha$  and  $\beta$  are fixed and such that  $\alpha + \beta = 1$ .

- (2) Let the system of elements be the positive real numbers (except zero) and let the composition  $a.b$  assign to the numbers  $a$  and  $b$  the number  $a.b = \sqrt{ab}$  (the geometric mean). More generally,  $a.b = a^\alpha b^\beta$  with  $\alpha + \beta = 1$ ,  $\alpha, \beta \neq 0$ . Here,  $a^\alpha = e^{\alpha \ln a}$ .
- (3) Let the system of elements be the points of the  $n$ -dimensional affine space. Let the composition  $a.b$  assign to the points  $a$  and  $b$  a point on the line  $\overline{ab}$  that divides this line by a certain proportion  $\alpha : \beta$  (e.g. the mean of the line  $\overline{ab}$ ).
- (4) Let the system of elements be the points of the  $n$ -dimensional projective space except the points on an  $(n-1)$  dimensional hyperplane  $E_{n-1}$  of this space<sup>1</sup>.

Then the point  $a.b$  shall be on the line  $ab$  such that the double proportion  $(a, b, a.c, b.c)$ , where  $c$  is the intersection point between the line  $ab$  and  $E_{n-1}$ , has a certain, fixed, value  $\chi$ .

If one introduces projective coordinates, if  $a_1, \dots, a_{n+1}; b_1, \dots, b_{n+1}$  are the coordinates of the points  $a$  and  $b$  and if  $A_i x_i = 0$ ,  $i = 1, \dots, n+1$  is the equation of  $E_{n-1}$ , then the point  $a.b = d$  has the projective coordinates

$$d_i = A_i(a_i b_t - \chi b_i a_t) \text{ where } i, t = 1, \dots, n+1$$

Showing that this is indeed a group follows easily from this formula; we will show a very simple method that can be used for this in section 2.

Before starting to give examples of finite distributive groups, i.e. groups with finitely many elements, we will discuss a characteristic property of distributive groups. In an associative group, there is always one element, the unit element with notation  $e$  for which it holds that  $a.e = e.a = a$  for each element  $a$  in the associative group. In an distributive group there is no such element, rather, there is a such *homogeneity* that any property of one element of this group holds for each element of this group (see section 2).

We want to show that any non-trivial distributive group (i.e. with more than one element) cannot include a unit element. If we set in one of the relations of Axiom III  $b = c = a$ , with  $a$

---

<sup>1</sup>*Dual*: Let the system of the elements be the  $E_{n-1}$  of a projective  $R_n$  except the  $E_{n-1}$  going through a certain point in  $R_n$ .

any element in the group, then we have  $(a.a).a = (a.a).(a.a)$  and hence, because of Axiom II the important relation

$$a.a = a$$

which thus holds for all elements in an distributive group. If now a unit element  $e$  were to be an element of this group, then we would have  $a.e = a.a$  and hence  $a = e$ , that is, every element in this group would be the unit element and hence the group would be trivial. *q.e.d.*

The trivial group with only one element  $a$  for which Axiom I holds via  $a.a = a$  is hence an example of a group which is both associative and distributive.

(Such a group can only have one element since otherwise it would not be distributive. On the other hand, in order to be associative it must include the unit element.)

*A distributive group with only two elements does not exist.* Let  $a$  and  $b$  be those two elements, then from  $a.a = a$  and  $b.b = b$  we get that  $a.b \neq a, b$  so that Axiom I does not hold.

*The distributive group with three elements exists.* In fact, it is commutative. Let  $a, b, c$  be the elements of this group, so we have that  $a.a = a$ ,  $b.b = b$  and  $c.c = c$ .  $a.b \neq a, b$  so  $a.b = c$  similarly,  $a.c = b$  and  $b.c = a$ . The Cayley table of this group is

	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

*Now we show that every finite commutative distributive group has odd order.* Let  $G\{a_1, a_2, \dots, a_n\}$  be a commutative distributive group of order  $n$ . We extract one element,  $a_1$ , say and have a closer look at the rest-system,  $a_2, \dots, a_n$ .

Let  $a_i$  be an element of this rest-system, then there exists an "assigned" element  $a_{\sigma_i}$  in  $G$  such that

$$a_i.a_{\sigma_i} = a_1$$

Since  $a_i \neq a_1$ ,  $a_{\sigma_i} \neq a_1, a_i$ . Thus,  $a_{\sigma_i}$  is an element of the rest-system which is not equal to  $a_i$ . Since the group is commutative,  $a_{\sigma_i}$  has  $a_i$  as its assigned element. Thus, the elements of the rest-system are paired in assigned element pairs and hence the order of the rest-system is even. Therefore, the order of  $G$  is odd, *q.e.d.*

*Conversely, for each odd number  $2N + 1$  there exists a commutative distributive group of this order.* We call the elements of this group  $1, 2, \dots, 2N + 1$  and let the composition element  $a.b$  of the elements  $a$  and  $b$  be as follows

$$a.b \equiv (n + 1)(a + b) \pmod{2n + 1}$$

It is easy to see that this is indeed a commutative group.

Geometrically, this is the group of vertices of a  $2n + 1$ -gon where the composition element  $c = a.b$  is then always lying on the perpendicular bisection of the line with endpoints  $a, b$ .

*Proof.* Since  $a(n + 1) \equiv \frac{a}{2} \pmod{2n + 1}$ , we can rewrite  $a.b$  as

$$a.b \equiv \frac{a + b}{2} \pmod{2n + 1}$$

Now let  $a < b$ . Then

1.

$$b = a + 2d, c \equiv \frac{2a + 2d}{2} = a + d \pmod{2n + 1}$$

that is,

$$c = a + d, b = c + d$$

2.

$$b = a + 2d + 1, c \equiv \frac{a + b + 2n + 1}{2} \equiv a + d + n + 1 \equiv b + (n - d) \pmod{2n + 1}$$

that is,

$$c = b + (n - d), c + (n - d) = b + 2(n - d) = a + 2n + 1 \equiv a$$

q.e.d.

Even though there are no commutative groups of even order, there are non-commutative ones. The *group of order four* is one example. If we let  $a_1, a_2, a_3, a_4$  be the elements of this group, we can always assume  $a_1.a_2 = a_3$  (since  $a_1.a_2$  can only be  $a_3$  and  $a_4$  and we can always renumber to get  $a_1.a_2 = a_3$ ). This means that in the Cayley table the following compositions are known:

	$a_1$	$a_2$	$a_3$	$a_4$
$a_1$	$a_1$	$a_3$	.	.
$a_2$		$a_2$		
$a_3$			$a_3$	
$a_4$				$a_4$

In the first row,  $a_2$  and  $a_4$  have to be in the two free places. Since  $a_4.a_4 \neq a_4$ ,  $a_1.a_3 = a_4$  and  $a_1.a_4 = a_2$ . With the help of Axiom II, one can fill in the other free places as well and this leads to:

	$a_1$	$a_2$	$a_3$	$a_4$
$a_1$	$a_1$	$a_3$	$a_4$	$a_2$
$a_2$	$a_4$	$a_2$	$a_1$	$a_3$
$a_3$	$a_2$	$a_4$	$a_3$	$a_1$
$a_4$	$a_3$	$a_1$	$a_2$	$a_4$

With this table, it is easy to show that Axiom III holds. Thus, there is one and only one distributive group of order four.

There is, again, only one group of order five, the commutative one described earlier, while there is no group of order six.

The question of classifying all groups of a given order seems to be as hard for distributive groups as is the equivalent question for associative groups. There will be more examples in section 3.

## 2. HOMOGENEITY OF DISTRIBUTIVE GROUPS

Let  $G$  be a distributive group and let  $A = \{a_1, a_2, \dots\}$  be a subgroup of  $G$  ( $A$  does not have to be countable. The notation  $a_i$  is chosen for simplicity). Let  $p$  be any element of  $G$ , then  $B = A.p = \{b_1 = a_1.p, b_2 = a_2.p, \dots\}$  is a subgroup of  $G$ , isomorphic to  $A$ .

Here, similarly to classical group theory, we call two groups  $\{a_1, a_2, \dots\}$  and  $\{b_1, b_2, \dots\}$  uniquely isomorphic<sup>2</sup> if a bijective map  $a_i \mapsto b_i$  can be defined such that to the composition  $a_i.a_k$  of  $a_i$  and  $a_k$  can be assigned a unique composition  $b_i.b_k$  of  $b_i$  and  $b_k$ , where  $b_i$  is assigned to  $a_i$  and  $b_k$  is assigned to  $a_k$ .

<sup>2</sup>In the original, *einstufig isomorph*. For a definition, see Definition A.2

*Proof.* If  $A$  is a finite group,  $a_i.a_k = a_l$  implies via a right-sided composition with  $p$ :  $b_i.b_k = b_l$ . The Cayley table of the system  $\{b_1, b_2, \dots\}$  is therefore the same as the Cayley table of the system  $\{a_1, a_2, \dots\}$  if the letter  $b$  is replaced with the letter  $a$ . Thus,  $B$  is a subgroup of  $G$ , isomorphic to  $A$ .

For infinite groups, the same proof holds via an extension of Cayley tables to infinite groups.

If  $A \cong G$ , the result is: If  $p$  is any element of  $G$ , then  $G$  is isomorphic to itself via the map  $a_i \mapsto a_i.p$ . *q.e.d.*

Due to Axiom II, we can always choose  $p$  such that (assuming  $a_i, a_k$  fixed)  $a_i.p = a_k$ . Thus,

*For any distributive group there exists a unique isomorphism such that a fixed element  $a_i$  gets mapped to  $a_k$ .* From this, the homogeneity of distributive groups follows.

*Every group theoretic property, which holds for at least one element in a distributive group, holds for all elements of this group.*

Conclusion 1: If an element  $a_i$  is an element of exactly  $h$  different subgroups of order  $v$  of a group  $G$ , then this holds for each element in  $G$ .

Thus, if  $G$ , a finite group of order  $N$ , has  $n$  different subgroups of order  $v$ , namely

$$A_1, A_2, \dots, A_n$$

then each element of  $G$  is an element of exactly  $h$  of those subgroups. Hence,

$$Nh = nv$$

Conclusion 2: Let  $G$  be a finite group of order  $N$ , let  $A_1$  be a subgroup of  $G$  with order  $v$  and let

$$A_2, A_3, \dots, A_m$$

be all the subgroups of  $G$  that are isomorphic to  $A_1$ . It is easily shown that all groups in the system

$$(1) \quad A_1, A_2, \dots, A_m$$

are pairwise isomorphic and hence  $A_i.p$  is isomorphic to  $A_i$  and thus to each  $A_j$ . Therefore,  $A_i.p$  is also an element of this system (1) of isomorphic subgroups.

Now if  $a_i$  is an element of  $q$  of those groups (1) then this holds for every element of  $G$ .

Counting all elements of  $G$  that are elements of groups in (1), we get

$$Nq = mv$$

*A closer look at the interesting case  $q = 1$ , for which the group  $G$  can be described via its subgroups in the system (1) as*

$$G = A_1 + A_2 + \dots + A_m$$

Now let  $A = A_i$ , for some  $i$ , then the union of the *different* subgroups of the union of

$$A.a, A.b, \dots, \text{ etc., where } G = \{a, b, \dots\}$$

is the same as the groups in (1).

This leads to the following proposition.

**Proposition 2.1.** *Let  $A, B$  be subgroups of  $G$  with  $B \neq A$ ,  $A \cong B$ . If  $A \cap B = \emptyset$ , then the following holds:*

$$G = A + A.\beta + A.\gamma + \cdots + A.\epsilon$$

*Considered as elements, the system of subgroups  $A, A.\beta, \dots$  is itself a distributive group  $\Gamma$  which is  $v$ -step isomorphic<sup>3</sup> to  $G$ .*

To properly understand this proposition, we have to explain the composition of two groups  $C \{c_1, c_2, \dots\}$  and  $D \{d_1, d_2, \dots\}$ . In particular,  $C.D$  is the system of all elements  $c_i.d_k$ ,  $i, k = 1, 2, \dots$

*Proof.* We now have to show Axiom I, that is  $A_i.A_k = A_l$ , i.e. a group in the system (1).

Let  $a_1^r, a_2^r, \dots, a_v^r$  be the elements of the group  $A_r$ ,  $r = 1, \dots, m$  and consider the two isomorphic groups

$$a_1^i.A_k \text{ and } A_i.a_l^k$$

both of which are elements of the system (1). Their intersection includes the element  $a_1^i a_l^k$  and both must therefore coincide. Thus we have

$$A_l = a_1^i.A_k = A_i.a_1^k = A_i.a_2^k = \cdots = A_i.A_k$$

and Axiom I holds.

In order to prove Axiom II, we have to show that the equation

$$A_i.X = A_l$$

has exactly one solution in the system (1).

Certainly, there is one element  $x = a_l^i$  in  $G$  such that  $a_1^i.a_l^i = a_l^i$ . This means, however, that  $A_i.A_k = A_l$ , that is,  $X = A_k$ . If there would be a second solution,  $A_j$ , say, that is  $A_i.A_j = A_l = A_k$ , this would imply that  $a_1^i.A_j = a_1^i.A_k$  and hence  $A_j = A_k$ . Thus, Axiom II holds. For  $Y.A_l = A_k$ , the proof is similar.

The proof of Axiom III is straightforward as well:  $(A_i.A_k).A_l$  and  $(A_i.A_l).(A_k.A_l)$  are groups in (1). Both groups include the element

$$(a_1^i.a_1^k).a_l^l = (a_1^i.a_l^l).(a_1^k.a_l^l)$$

and do therefore coincide.

*q.e.d.*

*We now give three examples of systems of isomorphic subgroups for which  $q=1$  holds.*

Example 1: Let  $G$  be a group of order  $N$  and let  $A$  be a subgroup of  $G$  of order  $v$ . Let  $A$  have the property that the intersection of  $A$  with any other subgroup of  $G$  of order  $v$  be empty. Then  $A$  is also disjoint to any subgroup of  $A$  which are isomorphic to  $A$  and Proposition 2.1 holds.

Example 2: Let  $G$  be a group of order  $N$  and let  $a_1 \in G$ . Then the elements  $x \in G$ , where

$$(2) \quad a_1.x = x.a_1$$

are elements of a subgroup  $A$  of  $G$  which is disjoint to any other isomorphic subgroup of  $G$ .

Since there are only finitely many solutions to equation (2), namely  $x = a_1, a_2, \dots$ , we only have to check Axiom I to show it is a group. In particular, since  $a_1.x = x.a_1$  and  $a_1.y = y.a_1$ , we have that  $a_1.(x.y) = (x.y).a_1$  that is, if  $x$  and  $y$  are a solution,  $x.y$  is a solution as well. Let  $A = \{a_1, a_2, \dots, a_v\}$  be the set of all solutions, then  $a_1$

---

<sup>3</sup>In the original *v-stufig isomorph*. For a definition, see Definition A.2

commutes with every other element in  $A$ . Indeed, for any element  $a_i \in A$ ,  $A$  is the subgroup of  $G$  of all elements that commute with  $a_i$ , since any element that commutes with  $a_i$  also commutes with  $a_1$ .

Now let  $B \cong A$ , another subgroup of  $G$ .  $B$  also has order  $v$  and, due to the homogeneity of the group  $G$ ,  $B$  includes all elements that commute with each other. Clearly, if  $A$  and  $B$  are not disjoint, they must be equal, since one element is enough to generate  $A$  and  $B$ , respectively. This proves the statement.

Example 3: First, let us introduce the following notation:

$$\begin{aligned} a.(a.b) &= a^2.b \\ a.[a.(a.b)] &= a^3.b \end{aligned}$$

Let  $G$  be a group of order  $N$  and let  $a_1 \in G$ . We claim: All elements  $x \in G$  with  $a_1^r.x = x$  constitute a subgroup  $A$  in  $G$  which is disjoint to any other subgroup of  $G$  which is isomorphic to  $A$ . The proof of this being a group is done similar as in Example 2. Let  $A$  be the group of solutions  $\{a_1, a_2, \dots, a_v\}$  and call  $r$  the *degree* of the group  $A$  of order  $v$ . Then, since  $a_1^r.a_i = a_i$  for  $i = 1, 2, \dots, v$  and due to the homogeneity of  $A$ , we have that  $a_i^r.a_i = a_i$  for  $i, t = 0, 2, \dots, v$ , that is,  $A$  is generated by any one of its elements. Similarly, if  $B = \{b_1, b_2, \dots, b_v\}$  with  $B \cong A$  and  $B$  a subgroup of  $G$ , then  $B$  is generated by any one of its elements  $b_i$  with  $b_i^r.x = x$ <sup>4</sup>. Thus, if  $A$  and  $B$  are not disjoint,  $A = B$ .

*Remark.* Instead of  $a_1^r.x = x$  we could have also used  $a_1.[(x.a_1).a_1] = x.a_1$  or indeed any other similar equation, as long as  $x$  only occurs once on each side.

### 3. PRINCIPLES OF THE GENERATION OF DISTRIBUTIVE GROUPS

**3.1. Generation from Associative Commutative Groups.** Let  $G_\alpha = \{a_1, a_2, \dots, a_{2n+1}\}$  be an associative, commutative group of order  $2n+1$ , let  $\alpha \in \mathbb{N}$  and let  $\alpha$  and  $\alpha-1$  be coprime with  $2n+1$  (for example  $\alpha = 2$  or  $\alpha = n+1$ ). The composition of the two elements  $a_i, a_k \in G$  shall we denoted by  $a_i \circ a_k$  and then the following holds:

$$a_i \circ a_k = a_k \circ a_i \text{ and } (a_i \circ a_k) \circ a_l = a_i \circ (a_k \circ a_l)$$

Furthermore,  $\alpha_i^\alpha = a_i \circ a_i \circ \dots \circ a_i$ , iterated  $\alpha$  times. For all  $g \in G_a$ , there is an  $i \in 1, \dots, 2n+1$  such that  $a_i^\alpha = g$ . This holds since if not, there is some  $i, k$  such that  $a_i \neq a_k$  with  $a_i^\alpha = a_k^\alpha$ . Let  $a_k^{-1}$  be the inverse element of  $a_k$  in  $G_a$ , then  $a_i^\alpha \circ (a_k^{-1})^\alpha = 1 = (a_i \circ a_k^{-1})^\alpha$ . However,  $a_i \circ a_k^{-1}$  cannot be the unit element, since otherwise  $a_k^{-1} = a_i^{-1}$ , that is  $a_i = a_k$  which is a contradiction. Now let  $a_l = a_i \circ a_k^{-1}$  then  $a_l^\alpha = 1$  for some  $\alpha$ , thus there must be a subgroup of  $G_a$  of order  $v$ , where  $v$  is a divisor of  $\alpha$ . However,  $v$  would then divide  $2n+1$  as well, which, contrary to the assumptions, means that  $\alpha$  and  $2n+1$  are not coprime. Hence, the equation  $x^\alpha = a_i$ , i.e.  $x = a_i^{\frac{1}{\alpha}}$  is uniquely solvable in  $G_a$ <sup>5</sup>. The same holds for  $\alpha-1$  instead of  $\alpha$ .

We will now show that we can understand the elements of  $G_a$  as the elements of a distributive group  $G_a$  of order  $2n+1$  if we use the following composition

$$a_i.a_k = a_i^\alpha \circ a_k^{1-\alpha}$$

<sup>4</sup>This is due to the homogeneity of  $G$  itself

<sup>5</sup>We can always find a  $\beta \in \{1, \dots, 2n+1\}$  such that  $a^{\frac{1}{\alpha}} = a^\beta$ . In fact, since  $a = a^{\alpha\beta}$ ,  $a^{\alpha\beta-1} = 1$ . Clearly, this holds for  $\alpha\beta-1 = 2n+1$  i.e. for  $\alpha\beta \equiv 1 \pmod{2n+1}$  and since  $\alpha$  and  $2n+1$  are coprime, such a  $\beta$  exists.

Axioms I and II hold true due to our assumptions so we only have to show that Axiom III holds.

We have

$$(a_i \cdot a_k) \cdot a_l = (a_i^\alpha \cdot a_k^{1-\alpha})^\alpha \circ a_l^{1-\alpha} = a_i^{\alpha^2} \circ a_k^{\alpha(1-\alpha)} \circ a_l^{1-\alpha}$$

as well as

$$(a_i \cdot a_l) \cdot (a_k \cdot a_l) = (a_i^\alpha \circ a_l^{1-\alpha})^\alpha \circ (a_k^\alpha \circ a_l^{1-\alpha})^{1-\alpha} = a_i^{\alpha^2} \circ a_k^{\alpha(1-\alpha)} \circ a_l^{1-\alpha}$$

Thus, Axiom III holds.

*Remark 1.* For the special, commutative group  $G_a$  of order  $2n+1$  whose elements are  $1, 2, \dots, 2n+1$  with composition  $a \circ b \equiv a + b \pmod{2n+1}$ ,  $a^\alpha = \alpha a$ , i.e.

$$a \cdot b \equiv \alpha a + (1 - \alpha)b \pmod{2n+1}$$

*Remark 2.* Let  $G_a$  be the infinite commutative group with the elements being  $\mathbb{R}$  and whose composition is  $a \cdot b = a + b$ . Then  $a \cdot b = \alpha a + \beta b$  with  $\alpha + \beta = 1$  is the composition of the respective distributive group.

*Remark 3.* Let  $A_a$  be a subgroup of  $G_a$  of order  $v$ , then  $v$  is coprime to  $\alpha$  and  $\alpha - 1$  since  $v$  divides  $2n+1$ . Let  $b_1, b_2, \dots, b_v$  be the elements of  $A_a$ , then this system together with the composition  $b_i \cdot b_k = b_i^\alpha \circ b_k^{1-\alpha}$  is a distributive group. Thus, all elements of the subgroup  $A_a$  of  $G_a$  constitute a subgroup  $A_d$  of a group  $G_d$ .

The elements

$$A_d \cdot p = \{b_1 \cdot p, b_2 \cdot p, \dots, b_v \cdot p\} = \{b_1^\alpha \circ p^{1-\alpha}, \dots, b_v^\alpha \circ p^{1-\alpha}\} = \{b_1^\alpha, \dots, b_v^\alpha\} \circ p^{1-\alpha} = A^\alpha \circ p^{1-\alpha}$$

of the distributive subgroup  $A_d \cdot p$  constitute a "sidegroup"<sup>6</sup>  $A_\alpha \circ p^{1-\alpha}$  of the subgroup  $A_A$  of  $G_a$ . Thus, if  $A_d \cdot p$  and  $A_d \cdot q$  have an element in common, they are in fact equal and the following decomposition holds:

$$(3) \quad G_d = A_d + A_d \cdot p + \dots + A_d \cdot t$$

Now let

$$\begin{aligned} b_i \cdot p &= b_i^\alpha \circ p^{1-\alpha} \in A_d \cdot p \\ b_j \cdot q &= b_j^\alpha \circ q^{1-\alpha} \in A_d \cdot 1 \end{aligned}$$

then

$$\begin{aligned} (b_i \cdot p) \cdot (b_j \cdot q) &= (b_i^\alpha \circ p^{1-\alpha})^\alpha \circ (b_j^\alpha \circ q^{1-\alpha})^{1-\alpha} \\ &= (b_i^\alpha \circ b_j^{1-\alpha})^\alpha \circ (p^\alpha \circ q^{1-\alpha})^{1-\alpha} \\ &= (b_i \cdot b_j) \cdot (p \cdot q) \end{aligned}$$

However, since this element is an element of  $A_d \cdot (p \cdot q)$ , the subgroups in (3) constitute, taken as elements, another distributive group (Axioms II and III hold with proof as before).

Furthermore, we have the following composition:

$$(b_i \cdot p) \cdot (b_j \cdot q) = (b_i \cdot b_j) \cdot (p \cdot q)$$

Let  $B_d = \{b_1, \dots, b_\mu\}$  and  $C_d = \{c_1, \dots, c_r\}$  be two subgroups of  $G_d$ . Then from

$$(b_i \cdot c_k) \cdot (b_j \cdot c_i) = (b_i \cdot b_j) \cdot (c_k \cdot c_i)$$

it follows that the elemental system

$$\{\dots, (b_i \cdot c_k), \dots\}, i = 1 \dots \mu, j = 1, \dots, r$$

---

<sup>6</sup>In the original *Nebengruppe* as compared to *Untergruppe*, which is a subgroup.



is a group.

### 3.2. Generation of Distributive Groups from Distributive Groups.

*Remark.* The same holds for associative Groups.

Let  $A = \{1_1, \dots, a_v\}$  and  $B = \{b_1, \dots, b_\mu\}$  with their respective compositions  $a_i \cdot a_k$  and  $b_i \odot b_k$  be two distributive groups of order  $v$  and  $\mu$ , respectively. Then the elemental system  $\{\dots, (a_i, b_k), \dots\}$  with the composition  $(a_i, b_k) \times (a_j, b_l) = (a_i \cdot a_j, b_k \odot b_l)$  is also a distributive group and has order  $v\mu$ . It is immediately clear that Axioms I to III hold.

A group that has been generated like this such that every element  $(a_i, b_k)$  is numbered by two indices shall be called *Double Index Group*<sup>7</sup>. Similarly, triple index groups and higher can be generated.

*Remark.* If the composition  $a \cdot b = a^\alpha \circ b^{1-\alpha}$  gets replaced by the composition  $a \cdot b = a^\alpha \circ b^\beta$ , where  $\alpha, \beta$  are coprime with  $2n + 1$ , then from the Cayley table it is clear that Axioms I and II hold. Instead of Axiom III, we have

$$(a \cdot d) \cdot (b \cdot d) = (a \cdot b) \cdot (d \cdot d), \text{ and } (d \cdot a) \cdot (d \cdot b) = (d \cdot d) \cdot (a \cdot b)$$

or more generally

$$(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d)$$

For those groups the relationship with abelian groups of odd order as outlined in this chapter hold.

If  $A$  is a subgroup, then  $A \cdot p$  is a "sidegroup", similarly as for associative groups.

## 4. SUBGROUPS, INDEX THEOREM

**Theorem 4.1.** *A group is called simple if it has no proper subgroup of order bigger than one. It follows that any simple group is completely described by any two of its elements.*

*Proof.* Let  $A = \{a_1, \dots, a_v\}$  be a simple subgroup of a group  $G$  and let  $p \in G$ . Then we will show that  $A \cdot (A \cdot p)$  is an  $r$ -class group *A.t.*<sup>8</sup> We denote the group  $A \cdot p$  with  $B = \{a_i \cdot p = b_i, i = 1, \dots, v\}$ . Then the following holds

$$a_i \cdot b_1 = a_i \cdot (a_1 \cdot p) = (a_i \cdot a_1) \cdot b_i = a_j \cdot b_i$$

where  $a_i \cdot a_1 = a_j$ .

Let  $a_i \neq a_1$ , then  $a_i \neq a_j$  and also  $b_i \neq b_j$ . The two groups  $a_j \cdot B$  and  $A \cdot b_1$  are uniquely isomorphic to  $A$ , so are simple as well.  $a_j \cdot b_1$  and  $a_i \cdot b_1 = a_j \cdot b_i$  are elements of both groups and so they are equal as simple groups, that is

$$A \cdot b_1 = a_j \cdot B, \text{ with } j = 2, 3, \dots, v$$

Similarly,

$$A \cdot b_2 = a_h \cdot B, \text{ with } h = 1, 3, 4, \dots, v$$

from which it follows that

$$a_1 \cdot B = a_2 \cdot B = \dots = a_v \cdot B = A \cdot B = A \cdot (A \cdot p)$$

*q.e.d.*

<sup>7</sup>In the original *Zweiindizesgruppe*

<sup>8</sup>In the original *r-gliedrige Gruppe*. A definition is provided in Definition A.4.

We now want to extend Theorem 4.1 to groups that are uniquely determined by exactly two of their elements (but not any two elements). First, we will show the following lemma.

**Lemma 4.2.** *Let there be such a subgroup  $A$  and let  $a_l, a_k \in A$  the two elements that determine  $A$ . Then if  $a_i.a_j = a_k$ , both  $a_i$  and  $a_j$  as well as  $a_k$  and  $a_j$  determine the subgroup, too.*

*Proof.*  $a_i$  and  $a_j$  determine a smallest group  $\bar{A}$  for which  $\bar{A} \leq A$  holds; but  $a_k \in \bar{A}$  and thus  $A \subset \bar{A}$ , that is  $\bar{A} \geq A$  and hence  $A = \bar{A}$ . *q.e.d.*

The same proof holds for  $a_k$  and  $a_j$ . We will now prove the theorem.

*Proof.* Let the group  $A$  be determined by its elements  $a_l$  and  $a_k$ . Furthermore, as above, we have

$$\begin{aligned} (4) \quad & a_i.a_j = a_k && \text{fixed, then} \\ (5) \quad & a_k.b_j = (a_k.a_j).b_k && \text{and} \\ (6) \quad & a_l.b_j = (a_i.a_j).b_l = a_k.b_l = (a_k.a_l).b_k. \end{aligned}$$

The uniquely isomorphic groups  $A.b_j$  and  $A.b_k$  both include the two elements  $a_k.b_j = (a_k.a_j)$  and  $a_i.b_j = (a_k.b_l).b_j$ .

The group  $A.b_j$  is uniquely determined by the two elements  $a_k.b_j$  and  $a_l.b.j$ ; similarly,  $(a_k.a_j).b_k$  and  $(a_k.a_l).b_k$  determine  $A.b_l$  uniquely. Thus,  $A.b_j = A.b_k$ .

Let  $x_1, x_2, \dots \in G$  be all the elements in  $G$  for which  $A.x_1 = A.x_2 = \dots A.b_j$  holds, then those elements constitute a subgroup of  $G$ . Since there are only finitely many such elements, we only have to show that Axiom I holds.

$$A.(x_p.x_q) \leq (A.x_p).(A.x_q) = (A.x_p).(A.x_p) = A.x_p = A.b_j$$

shows this group property. Since both  $b_j$  and  $b_k$  are also in this group and hence  $B$  is, we have

$$A.b_1 = A.b_2 = \dots = A.b_v = A.B$$

*q.e.d.*

**Proposition 4.3.** *Let  $A = \{a_1, a_2, \dots, a_v\}$  be a subgroup with the property that for any two elements  $a_i, a_k \in A$ , the equation  $a_i = a_k^2.a_i$  does not hold. Then  $A.(A.p) = A.t$ .*

We will use equations (4), (5) and (6).

*Proof.* Let  $k = 1, 2, \dots, v$ , then  $a_k.b_j = (a_k.a_j).b_k$  and  $a_i.b_j = (a_k.a_i).b_k$  are both elements in  $A.b_j$ . Thus, their product  $a_i.a_k).b_j = [a_k.(a_i.a_j)] = (a_k.a_k).b_k = a_k.b_k$  is also in  $A.b_j$ .

Hence, each of the elements

$$(7) \quad a_1.b_1, a_2.b_2, \dots, a_v.b_v$$

is an element of each of the groups  $A.b_j$ .

If all of the elements in (7) are distinct, then they determine uniquely the group  $A.b_j$  and  $A.b_1 = A.b_2 = \dots = A.b_v = A.B$  holds.

Let us take a closer look at

$$(8) \quad a_r.b_r = a_l.b_l$$

There exists an  $a_k \in A$  for which

$$(9) \quad a_r.a_k = a_l$$

holds. Thus,

$$\begin{aligned} a_r.b_k &= (a_r.a_k).b_r = a_l.b_r \\ &= (a_l.a_r).b_l = (a_l.b_l).(a_r.b_l) \\ &= (a_r.b_r).(a_r.b_l) = a_r.(b_r.b_l) \end{aligned}$$

from which  $b_k = b_r.b_l$  follows and hence

$$(10) \quad a_k = a_r.a_l$$

From (9) and (10) we conclude that  $a_l = a_r.(a_r.a_l) = a_r^2.a_l$ . Similarly,  $a_r = a_l^2.a_r$ .

However, this is a contradiction to the assumptions, so we have that  $A.(A.p) = A.t$ . *q.e.d.*

*Remark.* We will show that (8) follows from  $a_l = a_r^2.a_l$ .

*Proof.* We set  $a_r.a_l = a_k$  which is equivalent to  $a_l = a_r.a_k$ . We now have

$$a_r.b_k = a_r.(b_r.b_l) = (a_r.b_r).(a_r.b_l)$$

as well as

$$a_r.b_k = (a_r.a_k).b_r = a_l.b_r = (a_l.a_r).b_l = (a_l.b_l).(a_r.b_l)$$

Comparing these gives us the result,  $a_r.b_r = a_l.b_l$ . *q.e.d.*

**Corollary.** *Let  $A = \{a_1, \dots, a_v\}$  be a commutative group without any subgroup of order three, then  $A.(A.p) = A.t$ .*

This follows directly from the preceding remark.

If there were be a composition  $a_j = a_i.(a_i.a_j)$ , then from  $a_i.a_j = a_k$  it follows that  $a_j = a_i.a_k$ . Furthermore,  $a_j.a_k = (a_i.a_k).(a_i.a_j) = a_i.(a_k.a_j)$  from which  $a_j.a_k = a_i$  follows, that is,  $a_i$ ,  $a_j$  and  $a_k$  constitute a subgroup of order three, a contradiction.

**Theorem 4.4.** *Let  $A$  be a subgroup for which  $A.(A.p) = A.t$  holds. Then*

$$G = A + A.p + A.q + \dots + A.w$$

We will show this by showing that two subgroups  $A.p$  and  $A.q$  are either identical or disjoint.

*Proof.* Let  $c$  be an element in the intersection of those two subgroups. Then,

$A.(A.p) = A.c$  and  $A.(A.q) = A.c$ , respectively and thus  $A.(A.p) = A.(A.q)$  and hence  $a_1.(A.p) = a_1.(A.q)$  and thus  $A.p = A.q$ . *q.e.d.*

*Remark.* We will now show for later use if we have a simple subgroup of order  $v$ ,  $A = \{a_1, a_2, \dots, a_v\}$ ,  $(A.p).A$  is also a  $v$ -class group  $t.A$ .

*Proof.* We have

$$(11) \quad (a_i.p).a_k = (a_i.a_k).(p.a_k) = a_l.(p.a_k) = (a_l.p).(a_l.a_k) = (a_l.p).a_k$$

where

$$(12) \quad a_i.a_k = a_l \quad \text{and}$$

$$(13) \quad a_l.a_k = a_h$$

Furthermore,

$$(14) \quad (a_l.p).a_h = (a_l.a_h).(p.a_h) = a_s.(p.a_h) = (a_s.p).(a_s.a_h) = (a_s.p).a_t$$

where

$$(15) \quad a_l.a_h = a_s \quad \text{and} \quad a_s.a_h = a_t$$

For  $a_s$  and  $a_t$  we calculate

$$(16) \quad \begin{cases} a_s = a_l.a_h = (a_i.a_k).(a_l.a_k) = (a_i.a_l).a_k \\ a_t = a_s.a_r = [(a_i.a_l).a_k].(a_l.a_k) = [(a_i.a_l).a_l].a_k \end{cases}$$

and thus the two simple groups  $(a_i.p).A$  and  $A.p.a_h$  have the following elements in common

$$(17) \quad (a_i.p).a_h \quad \text{and} \quad (a_i.p).a_k = (a_l.p).a_h$$

Let  $A_i \neq a_k$ , then because of (12) we have that  $a_k \neq a_l$ . Then, by (13),  $a_h \neq a_k$ , which means the two elements in (17) are different. This leads to

$$(a_i.p).A = (A.p).a_h$$

with  $a_i.a_k = a_l$ ,  $a_l.a_k = a_h$ , that is  $(a_i.a_k).a_k = a_h$ .

Now there are two possible cases.

Case 1: For two values  $a_k$  ( $a_k$  and  $a_{\bar{k}}$ ) let  $a_h \neq a_{\bar{h}}$ . Then we have

$$(A.p).a_h = (A.p).a_{\bar{h}} = (A.p).A$$

Case 2: Let  $a_h$  be independent from  $a_k$  in  $a_h = (a_i.a_k).a_k$  for all  $k \neq i$ . Then it must that  $a_h = a_i$ , since if otherwise  $a_h = a_t$ ,  $t \neq i$ , we would have  $a_t = (a_i.a_t).a_t$  that is,  $a_i.a_t = a_t$  from which it follows that  $t = i$  which is a contradiction. Thus, the following must hold:

$$(18) \quad a_i = (a_i.a_k).a_k$$

Since  $a_i$  was arbitrary, equation (18) must hold for any two elements in  $A$  (otherwise it would be Case 1). But then it follows from equation (16) that  $a_t = a_i.a_k$  and the two simple  $(a_i.p).A$  and  $(A.p).a_i$  both include the two distinct elements  $(a_i.p).a_t$  and  $(a_i.p).a_k = (a_s.p).a_t$ . (Since  $a_t \neq a_k$  if  $a_i \neq a_k$ .) Thus, it follows that

$$(19) \quad (a_i.p).A = (A.p).a_t$$

If  $k$  is running through  $1, 2, \dots, i-1, i+1, \dots, v$ , then  $t$  runs through the same numbers (possibly in changed order), that is

$$(a_i.p).A = (A.p).a_1 = (A.p).a_2 = \dots = (A.p).a_v$$

since  $a_i$  was arbitrary.

*q.e.d.*

**Proposition 4.5.** *Let  $A = \{a_1, \dots, a_v\}$  be a subgroup with the property that for any two elements the following equations do not hold:*

$$\begin{aligned} (a_i.a_p).a_p &= a_i \\ (a_p.a_i).a_p &= a_i \end{aligned}$$

*Then  $(A.p).A = t.A$ .*

*Proof.* We are following equations (11) to (16).

The group  $(a_i.p).A$  includes the elements  $(a_i.p).a_h$  and  $(a_i.p).a_k = (a_l.p).a_h$  as well as all of the elements  $(x_r.p).a_h$  where  $x_r$  is any element of the smallest group with elements  $a_i, a_l, \{a_i, a_l\}$ . This group also includes the elements  $a_k, a_h, a_s, a_t$  and so  $(a_h.p).a_h \in (a_i.p).A$  with  $a_h = (a_i.a_k).a_k$ .

We claim that, together with  $a_k, a_h$  runs through all elements of  $A$ . From  $(a_i.a_k).a_k = (a_i.a_p).a_p = a_r$  we conclude as follows:

Set  $a_i.a_k = a_l$  and  $a_i.a_p = a_q$ , then  $a_l.a_k = a_q.a_p$ ; furthermore  $a_l.(a_p.a_k) = (a_i.a_k).(a_p.a_k) = (a_q.a_k)$ . In addition,

$$\begin{aligned} a_i.(a_p.a_k) &= (a_i.a_p).(a_l.a_k) = (a_l.a_p).(a_q.a_p) \\ &= (a_l.a_q).a_p = [a_i.(a_k.a_p)].a_p \\ &= a_q.[(a_k.a_p).a_p] \end{aligned}$$

Comparing gives  $a_k = (a_k.a_p).a_p$  which is a contradiction. Hence,  $(a_i.p).A$  includes all elements

$$(20) \quad (a_1.p).a_1, (a_2.p).a_2, \dots, (a_v.p).a_v$$

Next, set  $b_t = a_t.p$ , then  $b_l.a_l = b_k.a_k$ .

If  $a_r.a_k = a_l$ , then we form

$$\begin{aligned} b_r.a_k &= (a_r.p).a_k = a_l.(p.a_k) \\ &= b_l.(a_l.a_k) = (b_l.a_l).(b_l.a_k) \\ &= (b_k.a_k).(b_l.a_l) = (b_k.b_l).a_k \end{aligned}$$

From this, it would follow that  $b_r = b_k.b_l$ , that is  $a_r = a_k.a_l$  or, equivalently,  $(a_k.a_l).a_k = a_l$ , again a contradiction. Thus, all groups  $(a_i.p).A$  include the different elements in (20) and the following holds:

$$(a_1.p).A = (a_2.p).A = \dots = (a_v.p).A = (A.p).A$$

*q.e.d.*

*Implications from Theorem 4.4.*

1. A group whose order is prime, is simple.
2. The order of a simple subgroup, the order of a subgroup that is uniquely determined by two elements and the order of a subgroup, where the equation  $a_i^2.a_k = a_k$  does not hold for any pair of elements, divides the order of the group.
3. For subgroups of a commutative group, whose order is not divisible by 3, the index theorem holds (the order of the subgroup is not a divider of the order of the group).

To finish this section, we note the following theorem.

**Theorem 4.6.** *If  $(A.p).A = t.a$ , then also  $A.(p.A) = A.t$ , since it is always true that  $(A.p).A = A.(p.A)$ .*

*Proof.* Let  $(a_i.p).a_k \in (A.p).A$ , then since

$$(a_i.p).a_k = (a_i.a_k).(p - a_k)$$

it is also an element of  $A.(p.A)$  and hence

$$(A.p).A \leq A.(p.A)$$

Let  $a_i.(p.a_k) = (a_i.p).(a_i.a_k) \in A.(p.A)$ , then it is also an element of  $(A.p).A$  and hence

$$(A.p).A \geq A.(p.A)$$

and thus

$$(A.p).A = A.(p.A)$$

*q.e.d.*

*Remark.* Let  $G = \{a_1, a_2, \dots, a_v\}$  be a distributive group where the equation  $(a_i.a_k).a_k = a_i$  does not hold for any  $a_i, a_k \in G$ . Then we define a new composition,

$$a_i \circ a_k = (a_i.a_k).a_k$$

For this new system, Axioms I and II hold as well as

$$\begin{aligned} (a_i \circ a_k) \circ (a_j \circ a_k) &= [(a_i.a_k).a_k] \circ [(a_j.a_k).a_k] = \{[(a_i.a_k).a_k] \cdot [(a_j.a_k).a_k]\} \cdot [(a_j.a_k).a_k] \\ &= \{[(a_i.a_j).a_k] \cdot [(a_j.a_k).a_k]\} \cdot [(a_j.a_k).a_k] \\ &= [(a_i.a_j).a_k] \cdot [(a_j.a_k).a_k] = \{[(a_i.a_j).a_j] \cdot a_k\} \cdot a_k \\ &= (a_i \circ a_j) \circ a_k \end{aligned}$$

On the other hand, the left-sided distributivity does generally not hold.

## 5. THE STRUCTURE OF DISTRIBUTIVE GROUPS

In this section, we assume that for each subgroup  $A$  of  $G$   $A.(A.p)$  and  $(A.p).A$  are subgroups of the same order as  $A$ . Equivalently,

$$\begin{cases} A.(A.p) = A.t \\ (A.p).A = A.(p.A) = A.\tau \end{cases}$$

As shown in section 4, a sufficient condition for this to hold is that for any  $x, y \in G$ , neither of the following two equations hold:

$$(x.y).y = x, (y.x).y = x, y.(y.x) = x$$

We will call those groups *distinguished groups*<sup>9</sup>.

*Notation.* A subgroup  $A.p$  is denoted by  $[A]$

**Lemma 5.1.** *If  $A, B$  and  $C$  are subgroups, all of order  $v$ , then if  $A.B = C$ ,*

$$B = [A], C = [A], A = [B], C = [B], A = [C], B = [C]$$

*Proof.* Since  $A.B = C$ ,  $C = [A]$ . Let  $A = (a_t)$ ,  $B = (b_t)$ ,  $C = (c_t)$ , with  $t = 1, 2, \dots, v$  be all the elements of the three subgroups.

There exists an element  $r \in G$  such that  $a_1.r = b_1$ . Then we have

$$C = A.B = A.b_1 = A.(a_1.r) = A.(A.r)$$

that is,  $B = [A]$ . Furthermore,  $a_1 = b_1.q$  for some  $q \in G$ . Then

$$C = A.B = a_1.B = (b_1.q).B = (B.q).B = B.(q.B)$$

and hence  $C = [B]$  and  $A = [B]$ .

Finally,  $A.C = A.[C] = A.\sigma$ , and thus, similarly as before,  $A = [C]$  and in the same way, from  $B.C = B.[B] = B.\tau$  it follows that  $B = [C]$ . *q.e.d.*

**Lemma 5.2.** *Let  $A, B$  and  $C$  be  $v$ -class subgroups of, then since  $A.B$  is a  $v$ -class subgroup,  $A = [C]$  and  $B = [C]$ , it follows that  $A.B = [C]$ .*

---

<sup>9</sup>In the original *ausgezeichnete Gruppe*

*Proof.* In fact, since  $A = C.\theta$  and  $B = C.\tau$ ,

$$A.B = (C.\sigma).(C.\tau) \geq C.(\sigma.\tau)$$

But since  $A.B$  has class  $v$ , it follows that  $A.B = C.(\sigma.\tau) = [C]$ .

*q.e.d.*

**Lemma 5.3.** *Let  $A_1, A_2, \dots, A_\sigma$  be  $v$ -class subgroups with the property that pairwise products  $A_i.A_k$ ,  $i, k = (1, \dots, \sigma)$  are also  $v$ -class groups. Looking at the span of all those subgroups with pairwise products, one gets the system  $A_1, A_2, \dots, A_{\sigma+\tau}$  with the property that the pairwise products  $A_i.A_k$ ,  $i, k = 1, 2, \dots, \sigma + \tau$  is also a  $v$ -class group.*

*Proof.* We only have to show that  $A_i.A_{\sigma+k}$ ,  $A_{\sigma+k}.A_i$  and  $A_{\sigma+h}.A_{\sigma+k}$ ,  $i = 1, 2, \dots, \sigma$ ,  $h, k = 1, 2, \dots, \tau$  are  $v$ -class groups.

Since  $A_i.A_p$  are a  $v$ -class group, it follows by Lemma 5.1 that  $A_i = [A_p]$ ,  $i, p = 1, \dots, \sigma$  and since  $A_i.A_k$  is a  $v$ -class group, it follows from Lemma 5.2 that

$$A_i.A_k = [A_p], \quad p, i, k = 1, 2, \dots, \sigma$$

Thus,  $A_{\sigma+k} = [A_i]$ , since  $A_{\sigma+k} = A_r.A_s$  by the assumption, and hence  $A_i.A_{\sigma+k}$  (and also  $A_{\sigma+k}.A_i$ ) is a  $v$ -class group.

From this we deduce that  $A_i = [A_{\sigma+k}]$ ,  $i = 1, \dots, \sigma$ ,  $k = 1, \dots, \tau$ . Now let  $A_{\sigma+h} = A_p.A_q$ , then  $A_p = [A_{\sigma+k}]$  and  $A_q = [A_{\sigma+k}]$  and since  $A_p.A_q$  is a  $v$ -class group, by Lemma 5.2  $A_p.A_q = A_{\sigma+h} = [A_{\sigma+k}]$  and thus indeed  $A_{\sigma+h}.A_{\sigma+k}$ ,  $h, k = 1, 2, \dots, \tau$  are groups of class  $v$ . *q.e.d.*

Now we can proof the following theorem.

**Theorem 5.4.** *Let  $A_1, A_2, \dots, A_\sigma$  be groups of class  $v$  with the property that any product  $A_i.A_k$ ,  $i = 1, 2, \dots, \sigma$  is also  $v$ -class, then we can generate a distributive group, where the elements are  $v$ -class subgroups. In addition,  $A_1, A_2, \dots, A_\sigma$  are elements in this group.*

*Proof.* We complete the system  $A_1, A_2, \dots, A_\sigma$  with those products  $A_i.A_k$  that are not included and get a new system  $A_1, \dots, A_{\sigma+\tau}$  that will be completed in the same and so on until we arrive at a system

$$(21) \quad A_1, A_2, \dots, A_\epsilon$$

which is closed under the products  $A_i.A_k$ . Since  $G$  is finite, such a system exists. In particular, since all groups  $A_k$ ,  $k = 1, 2, \dots, \epsilon$  will have the form  $A_k = [A_1]$  since  $A_i.A_k$  is  $v$ -class and are therefore disjoint<sup>10</sup>. Thus, Axiom I holds for the system (21).

Now let  $A_i$  be a subgroup of (21), then

$$A_i.A_k \text{ and } A_k.A_i, \text{ respectively, with } k = 1, 2, \dots, \epsilon$$

runs through all elements of the system (21) since from

$$A_i.A_k = A_i.A_j$$

it follows that

$$A_1^i.A_k = A_1^i.A_j$$

and hence  $A_k = A_j$ , which proves that Axiom II holds.

Finally, we will show one of the two relations of Axiom III, e.g.

$$(A_i.A_k).A_j = (A_i.A_j).(A_k.A_j)$$

---

<sup>10</sup>see Theorem 4.1

The groups  $(A_i.A_k).A_j$  and  $(A_i.A_j).(A_k.A_j)$  are elements of the system (21) by Axiom I and they are in fact identical, since both include the element  $(a_1^i.a_1^k).a_1^j = (a_1^i.a_1^j).(a_1^k.a_1.j)$ , which proves the Theorem. q.e.d.

As an application, we add the following corollary.

**Corollary.** *One can always build a distributive group from  $A$  and  $A.p$ , whose elements are subgroups of the form  $A.h$  and of which  $A$  and  $A.p$  are elements.*

In fact,  $A_1 = A$  and  $A_2 = A.p$  fulfil the assumptions of Theorem 5.4.

**Definition 5.1.** Let  $G$  be a group, then we call a subgroup  $A$  of  $G$  a *maximal subgroup* if  $G$  is completely described by the elements  $a_1, a_2, \dots, a_v$  of  $A$  and another element  $p \in G - A$  in the complement of  $A$  in  $G$ . We denote this by  $\{A, p\}$ . Equivalently,  $G$  is the smallest group such that  $a_1, a_2, \dots, a_v, p \in G$ .

Then  $G \geq A + A.q_1 + A.q_2 + \dots + A.q_\sigma$ ,  $p \in A.q_1$  and since  $\{A, p\}$  must be the same  $G$  we have  $G = A + A.q_1 + \dots + A.q_\sigma$ .

Now set  $A = G_1$ , then the analogous holds for the maximal divider<sup>11</sup>  $A_1$  of  $G$ :

$$A = A_1 + A_1.r_1 + A_1.r_2 + \dots + A_1.r_l$$

We can keep reducing like this, until we arrive at a simple group (which does not have a divider and hence no maximal divider). This is because every finite group must have a maximal divider, which is of order 1 for simple groups.

To show this, let  $A$  be a subgroup of  $G$  and let  $\{A, p\} \neq G$ <sup>12</sup>. Then  $\{A, p\} = A_1 > A$  is a proper subgroup of  $G$ . Then  $\{A_1, p_1\}$  is either  $G$  or again a proper divider  $A_2$  of  $G$ , and so on.

Since  $G$  is finite, this must eventually end.

**Addendum 1.**<sup>13</sup> We denote the complex

$$(22) \quad (A.p).(A.q)$$

where  $A$  is a simple group, with  $H_{pq}$ . All the following theorems for the complex  $H_{pq}$  also hold in the case  $H_{pq} = A.(p.q)$ .

**Theorem 5.5.**  $H_{pq}$  has either  $v$  or  $v^2$  elements, where  $v$  is the order of  $A$ .

*Proof.* We will show that if  $H_{pq}$  has  $t < v^2$  elements then  $t = v$ . If  $t < v^2$ , then there are two elements  $(a_h.p).(a_k.q)$  and  $(a_{\bar{h}}.p).(a_{\bar{k}}.q)$ , where  $h \neq \bar{h}$  and  $k \neq \bar{k}$ , of the form

$$(23) \quad (a_h.p).(a_k.q) = (a_{\bar{h}}.p).(a_{\bar{k}}.q)$$

But then by Theorem 4.1

$$(24) \quad (A.p).(a_k.q) = (A.p).(a_{\bar{k}}.q)$$

holds. But since  $k \neq \bar{k}$  and since  $A.p$  is uniquely determined by two elements, it follows from (24) that

$$(25) \quad (A.p).(a_1.q) = (A.p).(a_2.q) = \dots = (A.p).(A.q) = A.(p.q)$$

Hence, in this case  $t = v$ .

q.e.d.

<sup>11</sup>In the original *Maximalteiler*.

<sup>12</sup> $\{A, p\}$  is the smallest subgroup of  $G$  with  $A$  and  $p$  as elements.

<sup>13</sup>We did not manage to prove that  $(A.p).(A.q)$  is a group of the same order as  $A$ . We do not know if this is correct or not. The theorems of the Addenda were proved during our attempts to prove this conjecture.



*Remark.* If  $H_{pq}$  has  $v$  elements, then  $H_{pq} = A.(p.q)$ . If  $H_{pq}$  has  $v^2$  elements, then

$$(26) \quad H_{pq} = (A.p).(a_1.q) + (A.p).(a_2.q) + \cdots + (A.p).(a_v.q)$$

**Theorem 5.6.**  $H_{pq}$  is a group.

*Proof.* Assume  $H_{pq}$  has  $v$  elements, then  $H_{pq} = A.(p.q)$  and is there a  $v$ -class group. Thus, we only have to show that  $H_{pq}$  is a group if it has  $v^2$  elements. From equation (26) it follows that

$$(27) \quad H_{pq} = (A.p).(a_1.q) + \cdots + (A.p).(a_v.q)$$

We denote the complex

$$(28) \quad [(A.p).(a_r.q)] \cdot [(A.p).(a_s.q)]$$

with  $K_{rs}$  and will show that it has less than  $v^2$  elements from which Theorem 5.5 implies it is a  $v$ -class group of the form

$$(29) \quad K_{rs} = (A.p).[(a_r.a_s).q] = (A.p).(a_t.q)$$

where

$$(30) \quad a_r.a_s = a_t$$

On the one hand,

$$(31) \quad [(a_t.p).(a_r.q)] \cdot [(a_t.p).(a_s.q)] = (a_t.p).[(a_r.a_s).q] = (a_t.p).(a_t.q) = q_t.(p.q)$$

but on the other hand,

$$(32) \quad [(a_r.p).(a_r.q)] \cdot [(a_s.p).(a_s.q)] = (a_r.a_s).(p.q) = a_t.(p.q)$$

From (31) and (32) it follows that  $K_{rs}$  has less than  $v^2$  elements, i.e. it is of the form (30). From (30) and (26),

$$(33) \quad H_{pq} > K_{rs}$$

i.e.  $H_{pq}$  is a group. *q.e.d.*

**Theorem 5.7.** For the group  $H_{pq}$  not only (26) holds but also

$$(34) \quad H_{pq} = A.\tau_1 + A.\tau_2 + \cdots + A.\tau_v$$

where  $\tau_1 = p.q$ .

*Proof.* We have  $A.p = A.(A.r)$  and  $A.q = A.(A.s)$  and hence

$$(35) \quad (A.p).(A.q) = [A.(A.r)] \cdot [A.(A.s)] \geq A.[(A.r).(A.s)]$$

But since

$$(36) \quad [a_l.(a_h.r)] \cdot [a_{\bar{l}}.(a_{\bar{h}}.s)] = [a_l.(a_h.r)] \cdot [a_{\bar{l}}.(a_{\bar{h}}.s)]^{14} = a_{\bar{h}}.[(a_h.r).(a_{\bar{h}}.s)]$$

it follows that

$$(37) \quad [A.(A.r)] \cdot [A.(A.s)] \leq A.[(A.r).(A.s)]$$

From (35) and (37) we get

$$H_{pq} = (A.p).(A.q) = A.[(A.r).(A.s)]$$

---

<sup>14</sup>There is always an element  $a_{\bar{h}}.s$  in all groups  $A.s$  for which  $a_{\bar{l}}.(a_{\bar{h}}.s) = a_l.(a_{\bar{h}}.s)$  holds, since  $A.(A.s)$  is a  $v$ -class group

and

$$(38) \quad H_{pq} = A.\sigma_1 + \cdots + A.\sigma_v = A.\tau_1 + \cdots + A.\tau_v$$

which is convincing once one chooses elements  $\sigma_i$  from  $(A.r).(A.s)$  one after another and takes into account that  $H_{pq}$  only has  $v^2$  elements. *q.e.d.*

**Theorem 5.8.** *If for a certain  $k$  in (34) and a certain  $l$  in (26) the following relation*

$$(39) \quad A.\tau_k = (A.p).(a_l.q)$$

*holds, then  $H_{pq}$  is of class  $v$  and vice versa.*

*Proof.* We will first prove the first part of the theorem. For this, call the average of the two complexes  $A$  and  $B$  with  $\vartheta(A.B)$ . Let  $H_{pq}$  be of class  $v$ , then for  $h = 1, 2, \dots, v$

$$(40) \quad \vartheta(A.\tau_1, (A.p).(a_h.1)) \geq a_h.(p.q)$$

since  $\tau_1 = p.q$ . Furthermore,  $A.\tau_k \neq A.\tau_1$  since  $\vartheta(A.\tau_k, (A.p).(a_h.q)) = 0$  for  $h \neq l$ .

However, since  $A.\tau_k = (A.p).(a_l.q)$ , then by (??) we would have

$$(41) \quad \vartheta(A.\tau_1, A.\tau_k) \geq a_l.(p.q)$$

This is a contradiction though, since all  $A.\tau_i$  are pairwise disjoint for  $i = 1, \dots, v$  (if  $H_{pq}$  has class  $v^2$ ). Thus,  $H_{pq}$  must be  $v$ -class.

The inverse is obvious<sup>15</sup>.

*q.e.d.*

**Corollary.** *If  $H_{pq}$  has  $v^2$  elements, then two subgroups  $A.\tau_k$  and  $(A.p).(a_l.q)$  have exactly one element in common.*

This follows from the two decompositions (26) and (34) since if they had two elements in common, both would be equal as simple groups and  $H_{pq}$  would be  $v$ -class.

**Theorem 5.9.** *From the relation*

$$(42) \quad \vartheta(H_{pq}, H_{pr}) \neq 0$$

*it follows that  $H_{pq} = H_{pr}$ .*

*Proof.* For  $H_{pq}$  and  $H_{pr}$  the following decompositions hold

$$(43) \quad H_{pq} = A.\tau_1 + \cdots + A.\tau_v \text{ and } H_{pr} = A.\sigma_1 + \cdots + A.\sigma_v, \text{ respectively.}$$

(where  $A.\tau_i$  are not necessarily all distinct. The same holds for  $A.\sigma_i$ ). So, by the assumption

$$(44) \quad (a_h.p).(a_k.q) = (a_{\bar{h}}.p).(a_{\bar{k}}.r)$$

from which we get

$$(45) \quad (A.p).(a_k.q) = (A.p).(a_{\bar{k}}.r)$$

We will now show that any group  $A.\tau_i$  from  $H_{pq}$  is identical with a group  $A.\sigma_j$  from  $H_{pr}$  if and only if  $H_{pq} = H_{pr}$ .

Let  $A.\tau_i$  be this group, so it has at least one element  $x$  in common with  $(A.p).(a_k.q)$ , and so, by (45), also by  $(A.p).(a_{\bar{k}}.r)$ . On the other hand, the latter group does have this element  $x$  in common with another  $A.\sigma_j$  from  $H_{pr}$ .

Thus,  $A.\tau_i$  and  $A.\sigma_j$  have the element  $x$  in common and are therefore equal.

*q.e.d.*

**Corollary.** *If an element  $a_i \in A$ ,  $A$  a group, is also an element in  $(A.p).l$ , then  $(A.p).l = A$ .*

---

<sup>15</sup>In the original *evident*.

*Proof.* In fact, since  $A.(A.p) = A.r$ , by Lemma 5.2,  $A = (A.p).s$ . The two complexes  $A.[(A.p).h] = [(A.p).s].[(A.p).l]$  and  $A.A = [(A.p).s].[(A.p).s] = A$  have the element  $a_i$  in common and are therefore identical. Since  $A.A$  has class  $v$ , the complex  $A.[(A.p).l]$  must also have class  $v$  and the following holds

$$A.[(A.p).l] = A.A = A$$

i.e.

$$(A.p).l = A$$

*q.e.d.*

**Theorem 5.10.** *For the subgroups in (34), the following relation holds*

$$(46) \quad (A.\tau_k).(A.\tau_l) = A.(\tau_k.\tau_l)$$

*Proof.* Since  $H_{pq}$  is a group,  $(A.\tau_k).(A.\tau_l) < H_{pq}$ . If  $(A.\tau_k).(A.\tau_l)$  would be  $v^2$ -class, then

$$(47) \quad (A.\tau_k).(A.\tau_l) = H_{pq}$$

but since  $(A.\tau_k).(A.\tau_k) = (A.\tau_k) < H_{pq}$  we would have

$$(48) \quad \vartheta [(A.\tau_k).(A.\tau_l), (A.\tau_k).(A.\tau_k)] = A.\tau_k$$

so by Theorem 5.9

$$(49) \quad (A.\tau_k).(A.\tau_l) = A.\tau_k$$

that is  $(A.\tau_k).(A.\tau_l)$  must be  $v$ -class which is a contradiction with the assumption that  $(A.\tau_k).(A.\tau_l)$  is  $v^2$ -class. Thus,  $(A.\tau_k).(A.\tau_l)$  must be  $v$ -class, i.e. equal to  $A.(\tau_k.\tau_l)$ . *q.e.d.*

Let  $G$  be a group and  $A$  be a simple subgroup of  $G$ , then the composition

$$(50) \quad G = A.l_0 + A.l_1 + \cdots + A.l_s, \text{ with } l_0 < A$$

holds. We remind us that  $A.(A.p) = A.t$  holds. Generally,  $(A.l_j).(A.p)$  is not necessarily  $v^2$ -class. The groups  $A.l_j$  with the property

$$(51) \quad (A.l_j).(A.l_h) = A.(l_j.l_h) \text{ for each } h = 0, 1, \dots, s$$

of which  $A$  is one of them shall be denoted by  $\widetilde{A.l_j}$ . Now let

$$(52) \quad \widetilde{A.l_0} = A, \widetilde{A.l_1}, \dots, \widetilde{A.l_r}$$

be the entirety of all those groups, then for them the following theorem holds.

**Theorem 5.11.** *The groups in (52) are elements of a distributive group  $\Gamma$ . Let  $\Sigma$  be the subgroup of  $G$  which includes all elements of  $G$  that are prevalent in elements of  $\Gamma$ .*

*Proof.* We will show

$$(53) \quad (\widetilde{A.l_k}).(\widetilde{A.l_h}) = \widetilde{A.(l_k.l_h)}$$

By the assumptions, we have

$$(54) \quad \begin{cases} (\widetilde{A.l_k}).(A.l_x) = A.(l_k.l_x) \\ (\widetilde{A.l_h}).(A.l_x) = A.(l_h.l_x) \end{cases}$$

so in particular,

$$(55) \quad (\widetilde{A.l_k}).(\widetilde{A.l_h}) = A.(l_k.l_h)$$

From (54) we deduce that  $\widetilde{A.l_k} = (A.l_x).p$  and  $\widetilde{A.l_h} = (A.l_x).q$  and thus  $(\widetilde{A.l_k}).(\widetilde{A.l_h}) = (A.l_x).(p.q)$ . We next have to show  $\widetilde{A.(l_k.l_h)}$ , i.e.  $[A.(l_k.l_h)].(A.l_x)$  is  $v$ -class. In fact,  $[A.(l_k.l_h)].(A.l_x) = [(A.l_x).(p.q)].(A.l_x)$  is also  $v$ -class. *q.e.d.*

**Theorem 5.12.** *Let  $G$  be a distinguished group,  $A$  a simple group of  $G$  of order  $v$  and let  $R$  be a subgroup of  $G$  which includes  $A$  of order  $v^2$ . If*

$$(56) \quad R = A.l_1 + A.l_2 + \cdots + A.l_v, \text{ with } l_1 < A$$

*is a composition via the group  $A$ , then  $A.l_h = \widetilde{A.l_h}$ ,  $h = 1, \dots, v$ .*

*Proof.* Let

$$(57) \quad G = R + R.p_1 + \cdots + R.p_t$$

From (56) it follows that

$$(58) \quad R.p_k = (A.l_1).p_k + \cdots + (A.l_v).p_k = (A.p_k).(l_1.p_k) + \cdots + (A.p_k).(l_v.p_k), \quad k = 1, \dots, t$$

We will show that  $R.p_k$  is of the form

$$(59) \quad R.p_k = A.s_1^{(k)} + \cdots + A.s_v^{(k)}$$

Since  $A.(A.p_k)$  is  $v$ -class, by Lemmata 5.1 and 5.2,  $A = (A.p_k).\sigma$ . Looking at the two complexes

$$(60) \quad A.(A.p_k) = [(A.p_k).\sigma].(A.p_k) \text{ and } A.[(A.p_k).(l_r.p_k)] = [(A.p_k).\sigma].[(A.p_k).(l_r.p_k)], \quad r = 1, \dots, v$$

They are both in the group  $R.(R.p_k) = R.p_l$ , therefore, by Theorem 5.9, they are either equal or both  $v$ -class. But since the first complex is  $v$ -class, the second one is as well and the group  $(A.p_k).(l_r.p_k) = (A.l_r).p_k$  is of the form  $A.s_v^{(k)}$ , i.e. we have

$$R.p_k = A.s_1^{(k)} + \cdots + A.s_v^{(k)}$$

If  $A.\tau$  is a subgroup of  $G$ , then by (57) and (59) it is equal to a subgroup  $A.s_r^{(k)}$ . By looking at the two complexes

$$(61) \quad A.(A.s_r^{(k)}) \text{ and } (A.l_k).(A.s_r^{(k)}), \quad k = 1, \dots, v$$

one can deduce in the same way as before that since  $A.(A.s_r^{(k)})$  is  $v$ -class,  $(A.l_k).(A.s_r^{(k)})$   $v$ -class so that  $A.l_k = \widetilde{A.l_k}$ . *q.e.d.*

**Theorem 5.13.** *Every distinguished group  $G$  is either identical with  $\Sigma^{16}$  or includes at least  $v$  subgroups  $\widetilde{A.l_k}$ .*

*Proof.* If for each  $(A.p)$  and  $(A.q)$ ,

$$(62) \quad (A.p).(A.q) = A.(p.q)$$

then  $G = \Sigma$ . If this is not the case, then there is at least one subgroup  $A.p$  so that  $(A.p).(A.q) = H_{pq}$  is  $v^2$ -class. Let  $l \in G$  such that

$$(63) \quad [a_1.(p.q)].l = a_i \quad a_1, a_i \in A$$

The group  $(H_{pq}).l$  includes  $A$ , by the Corollary to Theorem 5.9, i.e.

$$(64) \quad (H_{pq}).l = A + A.\sigma_1 + \cdots + A.\sigma_{v-1}$$

---

<sup>16</sup>i.e. every subgroup  $A.p$  of the group  $G$  is a  $\widetilde{A.p}$  subgroup

Thus,  $(H_{pq}).l$  has the properties of the group  $R$  of Theorem 5.12, that is

$$A.\sigma_k = \widetilde{A.\sigma_k}, \quad k = 1, 2, \dots, v$$

*q.e.d.*

*Remark.* If  $G$  is a distinguished group of order  $N$ , with  $N = \prod_{i=1}^n p_i$  where  $p_i$  are prime numbers with  $p_i \neq p_k$  for  $i \neq k$ , then for  $G$  the following relation holds for  $G$

$$(65) \quad (A, p).(A, q) = A.(p, q)$$

for all simple subgroups  $A$  of  $G$ .

In fact, if that would not hold true, then  $(A, p).(A, q) = H_{pq}$  be a  $v^2$ -class group. Since  $G$  is a distinguished group, then by Theorem 4.1  $v^2$  must divide  $N$  which is a contradiction. Thus, (65) holds. But if (65) holds for all simple subgroups of  $G$ , then it holds for all subgroups of  $G$ , which is easy to show.

Since every symmetric distributive group  $G$  of order  $N = \prod_{i=1}^n p_i$ , with  $N$  not divisible by 3, is a distinguished group, (65) holds for all symmetric groups.

## Addendum 2.

*A bit about the structure of distributive groups.* Let  $G = \{a_1, a_2, \dots, a_v\}$  be a distributive group, then from any two elements  $a_1$  and  $a_2$  we can create the following  $l$ -cycle (*left cycle*)  $a_1.a_2 = a_3, a_1.a_3 = a_4, \dots, a_1.a_{h-1} = a_h$ . All  $a_1, a_2, \dots, a_h$  shall be different while  $a_1.a_h$  should be equal to one of  $a_1, a_2, \dots, a_h$ .

$a_1.a_h$  must be different to both  $a_1$  and  $a_h$ , so if  $a_1.a_h = a_i$ ,  $i > 1$  and we claim that  $i = 2$ ; if  $i > 2$ , then from  $a_1.a_h = a_i$ ,  $a_h = a_1.a_{h-1}$  and  $a_i = a_i.a_{i-1}$  it would follow that  $a_1.a_{h-1} = a_{i-1}$ ; thus, already  $a_1.a_{h-1} = a_h = a_{i-1}$  would be equal to one of  $a_1, a_2, \dots, a_{h-1}$  which is a contradiction.

Thus, the cycle looks as follows:

$$(66) \quad a_1, a_2, a_3 = a_1.a_2, a_4 = a_1.a_3, \dots, a_h = a_1.a_{h-1}, a_2 = a_1.a_h$$

We also get the following relation between  $a_1$  and  $a_2$ :

$$a_1^{h-1}.a_2 = a_2$$

The equation  $a_1^{h-1}.x = x$  holds for the elements of a subgroup which includes the elements of the cycle (66).

Furthermore, the following relation exists between any two elements of this subgroup,

$$a^{h-1}.b = b, \text{ so in addition, } a_2^{h-1}.a_1 = a_1 \text{ and so on.}$$

**Definition 5.2.** We call  $h - 1$  the *degree* of the  $l$ -cycle  $a_1, a_2$ . Let  $A = \{a_1, a_2, \dots, a_v\}$  be a simple group, then the degree  $G$  of the  $l$ -cycle of any two elements  $a_p, a_q$ ,  $p \neq q$  is a characteristic invariant of this simple group, i.e. it is independent of the choice of  $a_p$  and  $a_q$ .

*Proof.* Any two elements  $a_p, a_q \in A$  have a certain  $l$ -degree  $g_{pq}$ ; since  $g_{pq}$  is a natural number, there must a smallest one. Let  $a_i, a_k$  be a combination whose cycle-degree is  $g$ , then  $a_i^g.a_k = a_k$ . The elements  $x$  that solve the equation  $a_i^g.x = x$ , constitute a subgroup of  $A$  which, since it includes both  $a_i$  and  $a_k$ , must necessarily be equal to  $A$ , since  $A$  is simple. Thus,

$$a_p^g.a_q = a_q \text{ for all elements of } A$$

i.e. any two elements  $a_p, a_q \in A$  have the cycle-degree  $g$ .

*q.e.d.*

Let  $A$  be a simple group of order  $N$  and  $l$ -cycle degree  $g$ . Then, using  $a_1$  and  $a_2$ , we generate the cycle

$$(67) \quad a_1, a_2, a_3 = a_1.a_2, \dots, a_{g+1} = a_1.a_g (a_2 = a_1.a_{g+1})$$

If not all elements in  $A$  have been included in this cycle, let  $a_{g+2}$  be such an element, not included in (67). We generate

$$(68) \quad a_1, a_{g+2}, a_{g+3} = a_1.a_{g+2}, \dots, a_{2g+1} = a_1.a_{2g} (a_{g+2} = a_1.a_{2g+1})$$

If  $a_i = a_{g+k}, i, k = 2, 3, \dots, g+1$ , then we would have that

$$a_1.a_i = a_i + 1 = a_1.a_{g+k})a_{g+k+1}$$

and finally  $a_{g+2} = a_l$ , a contradiction. Thus, apart from  $a_1$ , (67) and (68) are disjoint.

If there are further elements of  $A$  which are neither in (67) nor (68), then we generate another cycle with  $a_1, a_{2g+2}$  until every element in  $A$  is in one cycle. Every cycle (67), (68), ... includes  $g+1$  elements and thus  $N = \sigma g + 1$ , with  $\sigma \in \mathbb{N}$  or, equivalently,

$$N \equiv 1 \pmod{g}$$

**Theorem 5.14.** *Let  $N$  be the order and  $g$  be the cycle degree of a simple group, then*

$$N \equiv 1 \pmod{g}$$

The same holds for the  $r$ -degree, the degree of the *right* cycle; we only have to consider the relation  $a_i \circ a_k = a_k.a_i$  instead of  $a_i.a_k$  for which the system  $A = \{a_1, a_2, \dots, a_v\}$  is a distributive group as well.

In general, the  $l$  degree is not equal to the  $r$  degree.

*Proof.* Let  $A = \{a_0, a_1, \dots, a_v\}$  be a system whose elements create only one cycle,

$$a_0, a_1, a_2 = a_0.a_1, a_3 = a_0.a_2, \dots, a_v = a_0.a_{v-1} (a_0.a_v = a_1)$$

We will show that right-sided distributivity follows from left-sided distributivity and Axioms I and II. Since homogeneity holds for such systems, it is sufficient to show that

$$(a_i.a_k).a_0 = (a_i.a_0).(a_i.a_k)$$

We denote with  $a_\varrho$  the element for which

$$a_0.a_1 = a_\varrho.a_0$$

holds. Via left-sided composition with  $a_0$  we get

$$(69) \quad \begin{cases} a_0.a_{[t]} = a_{[\varrho+t-1]}.a_0, & a_{\varrho+t-1} = a_k \text{ fixed}, t = k+1-\varrho \\ a_0.a_{[k+1-\varrho]} = a_{[k]} \end{cases}$$

where  $[i]$  is the element for which

$$[i] \equiv i \pmod{v}$$

holds. Now, it follows from (69) and (68) that

$$\begin{aligned} (a_t.a_0).(a_s.a_0) &= [a_0.a_{[t+1-\varrho]}] \cdot [a_0.a_{[s+1-\varrho]}] = a_0 \cdot [a_{[t+1-\varrho]} - a_{[s+1-\varrho]}] \\ &= a_0.a_\mu = a_{[\varrho+\mu-1]}.a_0 \end{aligned}$$

where

$$a_\mu = a_{[t+1-\varrho]} \cdot a_{[s+1-\varrho]}$$

Composed left-sided  $(\varrho - 1)$  times with  $a_0$ , this give

$$a_t \cdot a_s = a_{[\mu + \varrho - 1]}$$

and so (68) becomes

$$(a_t \cdot a_0) \cdot (a_s \cdot a_0) = (a_t \cdot a_s) \cdot a_0$$

*q. e. d.*

#### APPENDIX A. TRANSLATED DEFINITIONS

In this section we will present the three definitions that are not used in the form of this paper anymore. We first give the German original definitions and then their respective translations. All the formatting and spelling has been copied exactly as in the originals.

The translations of the, now obsolete, "names" has been chosen to be as close as possible to their meaning in German. It is, however, not a literal translation. Should a reader recall the correct translation, we would be grateful if they could send a short note to the translator.

**A.1. Isomorphismen.** This part is taken from [2], Chapter 1 part 11, *Isomorphismen* [isomorphisms].

**Definition A.1.** Sind  $\mathfrak{F}$  und  $\mathfrak{F}'$  zwei Gruppen, und ist jedem Element  $F$  aus  $\mathfrak{F}$  ein bestimmtes Element  $F' = I(F)$  aus  $\mathfrak{F}'$  so zugeordnet, dass stets

$$I(F_1)I(F_2) = I(F_1 F_2)$$

ist und durchläuft dabei  $F'$  alle Elemente von  $\mathfrak{F}'$  wenn  $F$  alle Elemente von  $\mathfrak{F}$  durchläuft, so heit die Gruppe  $\mathfrak{F}'$  isomorph zu  $\mathfrak{F}$  und die Abbildung selbst ein Isomorphismus. Entspricht hierbei zu jedem Element  $F'$  auch nur ein einziges Element  $F$ , so heisst  $\mathfrak{F}'$  zu  $\mathfrak{F}$  einstufig isomorph, anderenfalls mehrstufig isomorph.

Translated, this becomes

**Definition A.2.** Let  $\mathfrak{F}$  and  $\mathfrak{F}'$  be two groups and let there be a mapping from each element  $F$  in  $\mathfrak{F}$  to each element  $F' = I(F)$  in  $\mathfrak{F}'$  for which

$$I(F_1)I(F_2) = I(F_1 F_2)$$

holds, and if  $F'$  runs through all elements of  $\mathfrak{F}'$  if  $F$  runs through all elements of  $\mathfrak{F}$ , then the group  $\mathfrak{F}'$  is isomorphic to  $\mathfrak{F}$  and the map  $I$  is an isomorphism. If for each element  $F'$  there is exactly one element  $F$ , then  $\mathfrak{F}'$  and  $\mathfrak{F}$  are *uniquely isomorphic*, otherwise *v-step isomorphic*.

**A.2. R-gliedrige Gruppe.** This part is taken from [3].

**Definition A.3.** Der Begriff einer *Gruppe von Transformationen*, welcher zunächst in der Zahlentheorie und in der Substitutionstheorie seine Ausbildung fand, ist in neuerer Zeit verschiedentlich auch für geometrische, resp. allgemeine analytische Untersuchungen verwendet worden. Man sagt von einer Schaar von Transformationen

$$x'_i = f_i(x_1, \dots, x_n, a_1, \dots, a_r)$$

(wobei die  $x$  die ursprünglichen, die  $x'$  die neuen Variablen (sic!) und die  $a$  Parameter bedeuten, die im folgenden stets *continuirlich* veränderlich gedacht werden), dass sie eine *r-gliedrige Gruppe* bilden, wenn irgend zwei Transformationen der Schaar zusammengesetzt wieder eine der Schaar angehörige Transformation ergeben, wenn also aus den Gleichungen

$$x'_i = f_i(x_1 \cdots x_n \alpha_1 \cdots \alpha_r)$$

und

$$x''_i = f_i(x'_1 \cdots x'_n \beta_1 \cdots \beta_r)$$

hervorgeht:

$$x''_i = f_i(x_1 \cdots x_n \gamma_1 \cdots \gamma_r)$$

unter den  $\gamma$  Grössen verstanden, die nur von den  $\alpha, \beta$  abhängen.

Translated, this becomes

**Definition A.4.** [...] A set of transformations

$$x'_i = f_i(x_1, \dots, x_n, \alpha_1, \dots, \alpha_r)$$

(where the  $x$  are the old,  $x'$  are the new variables and the  $\alpha$  are parameters which are thought to be continuous) constitutes a *r-class group* if the composition of any two transformations in this set is also in this set, that is if from the equations

$$x'_i = f_i(x_1, \dots, x_n, \alpha_1, \dots, \alpha_r)$$

and

$$x''_i = f_i(x'_1, \dots, x'_n, \beta_1, \dots, \beta_r)$$

it follows that

$$x''_i = f_i(x_1, \dots, x_n, \gamma_1, \dots, \gamma_r)$$

with parameters  $\gamma$  that only depend on  $\alpha, \beta$ .

#### REFERENCES

- [1] C. Burstin and W. Mayer, *Distributive Gruppen von endlicher Ordnung.*, J. Reine Angew. Math. **160** (1929), 111–130, DOI 10.1515/crll.1929.160.111 (German).
- [2] Kurt Reidemeister, *Einführung in die kombinatorische Topologie.*, 1932 (German).
- [3] Sophus Lie, *Ueber Gruppen von Transformationen*, Nachrichten von der Königl. Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen **1874** (1874), 529-542 (German).

Translated by ANSGAR WENZEL, UNIVERSITY OF SUSSEX, A.WENZEL@SUSSEX.AC.UK